Cybersecurity and the future of agri-food industries

by

Henry Okupa

B.S., Rivers State University of Science &
Technology, Nigeria, 1983

A THESIS

Submitted in partial fulfillment of the requirements

for the degree

MASTER OF AGRIBUSINESS

Department of Agricultural Economics

College of Agriculture

KANSAS STATE UNIVERSITY

Manhattan, Kansas

2020

Approved by:

Major Professor
Vincent Amanor-Boadu

ABSTRACT

The agri-food sector has been undergoing rapid changes in the areas of food production and distribution over the past decades. Over the years, the sector has moved from disconnected, independent and uncoordinated operations to a highly interconnected, dependent and coordinated operations that have enhanced efficiency. The principal cost of this highly efficient system of production is the increased complexity and the exposure to potential risks networked organizations face in the age of the fourth industrial revolution. Increasingly, the physical value of the agri-food sector's activities has declined even as the intangibles (data, information, insights) have increased in value. As precision agriculture becomes the mainstream and global positioning systems and RFIDs are deployed to enhance traceability and safety, the importance of data protection and security also become exponentially critical to the integrity of the system. That the sector is ahead of the general economy in the adoption of autonomous machines and artificial intelligence implies that the crucial valuation in the sector would be on data generation, organization and analytics, and machine learning. The combined complexity of these systems and processes interacting together create value and at the same time exposes the industry to significant operational risks. For while it was much difficult for cows and grains of corn to be stolen, stealing the data supporting the value embedded in these commodities is becoming increasing easy and riskier.

This research is an exploratory excursion into developing an awareness of the scope of the potential risks creeping into the agri-food sector. It raises concern about the nature, typology and structure of these cybersecurity risks, that identifies the skills and capabilities

that are needed for the sector to continue producing value to its customers even as it sustains its competitiveness. It focuses attention on building the internal capacities along the agri-food supply chain to ensure that all stakeholders have the appropriate capabilities and capacities to address the impending and emerging challenges. After all, every chain is as strong as its weakest link. Cybersecurity threat has become a very critical challenge facing all businesses. And the agri-food sector is not immune to the threats it presents. Being prepared is a necessary condition for securing the sector's future.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGMENTS

I would like to thank the staff and members of the Masters of Agribusiness Program at Kansas State University for all their time, support and efforts in ensuring that the program was successful. A very special thanks to Deborah Kohl and Mary Bowen for all they do and all their encouragements. Thank you to Dr. Featherstone for his dedication and commitment to the Master of Agribusiness Program (MAB). Thanks also to my classmates of class 2020, for been part of this journey.

A very sincere thanks to my Major Professor, Dr. Vincent Amanor-Boadu, who guided me all through this thesis. Thank you for your time, patience, strategic approach to problem solving and assistance in helping me to articulate clearly, and more. You are well appreciated, and I am indeed very grateful for the counsel.

I also would like to thank Dr. Beth Yeager for her tireless assistance when I needed it most, and for being part of my committee. Special thanks to Dr. Kara Ross for being part of my thesis committee, and for her kindness in willing to help.

Finally, I would like to give my sincerest gratitude to my wife, Weyimi, and my daughter, Ivana. Their support and understanding were never in short supply. Their willingness to encourage me never waned throughout the program.

CHAPTER I: INTRODUCTION

About 25 years ago, a new wave swept the world: information age was born. From entertainment to work, communication to industry, information gained currency and began to become critical to the competitiveness of business organizations (Mata, Furest and Barney 1995). It is important to recognize that the information age did not begin in the 1990s. Rather, it was the deployment of technology to facilitate the application of existing information, that enabled the development of new data, which could be transformed into new information, that created the novel opportunities that became part of the competitiveness structure of organizations. One of the major changes that happened with the information revolution was the migration of corporate and personal information from filing cabinets to cyberspace – servers that could be several thousand miles away from companies' physical locations.

The development of rapid deposit and retrieval technologies enabled the embedded transaction costs associated with the adoption and use of these technologies to fall rapidly through the years. The effect of this lowering of cost of use was massive adoption. Slowly, technologies that were previously only available to large, well-resourced organizations, became available to everyone, including individuals in their homes. They became available globally, allowing Chinese firms to provide near real-time service to their US clients, and Indian software developers to work on projects in the US as if they lived there. Information technology became the leveler in a world of massive inequalities.

As more companies jumped on the information revolution bandwagon, the inherent risks and opportunities associated with new technologies and massive adoptions began to

emerge. As expected, the focus in the early days was on building and improving these novel communication technologies that allowed massive transfer of data from one organization to another at virtually no costs across organizations in very distant locations. Little thought was put into the potential risks that would become obvious to any individual or organization who sought to exploit the weaknesses of the technologies for profit or power. As the technology became more universal, questions of privacy protection, data security and "viruses" and "malware" became more rampant. A new term emerged in the business lexicon: cybersecurity.

1.1 Cybersecurity Defined

It is important to note that curiosity was the foundation of a lot of the tools that later became part of criminal activity in cyberspace. Cybersecurity is reputed to have its origin in a research project done by Bob Thomas, who observed that it was possible for a computer program to move across computer networks while leaving a small trail along the way. To test his idea, Thomas wrote a program he christened Creeper, and served between Tenex terminals on the early ARPANET, printing the message "IM CREEPER: CATCH ME IF YOU CAN." Ray Tomlinson, the inventor of email, saw Thomas' Creeper and liked it, tinkered with it and gave birth to the first computer worm when he made the Creeper self-replicating. Tomlinson then wrote the first antivirus program to deal with the problem he has contributed to creating and called it Reaper. Reaper's job was to chase Creeper and delete it. It was all brilliant people exploring the limits of the emerging technology. No harm intended. As noted by SentinelOne (2019), "It's funny to look back from where we are now, in an era of ransomware, fileless malware, and nation-state

attacks, and realize that the antecedents to this problem were less harmful than simple graffiti."

A German computer hacker, Marcus Hess, hacked an internet gateway in Berkeley in 1986, using it to piggyback on the ARPANET, which allowed him to hack 400 military computers, including Pentagon mainframes. This was not a research project: Hess' intent was to sell the information to the KGB, the Russian intelligence agency. It needs to be acknowledged that the Russians had recognized the potential of the emerging internet technology as a potential weapon in cyber warfare. Astronomer Clifford Stoll detected the intrusion and deployed a honeypot technique, which led to catching Hess. Computer viruses and worms were becoming less of academic research activities and pranks and were quickly evolving into serious threat. Increasing network connectivity made the potential threat presented by those with criminal intent in this field more dangerous. For example, an early computer worm, the Morris, nearly wiped out the early internet, giving birth to the creation of the antivirus software industry. It is important to note that the author of what became known as the Morris worm did not have any criminal intent. He wanted to gauge the size of the internet, and his program was meant to propagate across networks, copying itself as it travelled. The program, which became known as the Morris worm, propagated so aggressively that it brought the early internet to a crawl, causing massive damage. Morris' "research" made him the first to be prosecuted under the Computer Fraud and Abuse Act, but it led to the formation of the non-profit US Computer Emergency Response Team, now housed within Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security with a $93 million budget (2013). From this simple beginning, thus

emerged a global computer virus and malware industry, which by 2014 was estimated to produce about half a million new and unique malwares were produced daily, up from the 5 million that was happening per annum in 2007. The biggest of these malwares to date was the WannaCry ransomware, which emerged on May 12, 2017 and within 24 hours infected more than 230,000 computers in 150 countries (SentinelOne 2019).

That is the brief history of factors and forces that have given birth to a novel industry in the age of networks, data transfers and Big Data activities at the personal and organizational levels around the world: Cybersecurity. What, then, is cybersecurity? Let us explore the definition and meaning of cybersecurity from its roots. Cyber comes from cybernetics, which has its roots in the Greek word *kubernētēs*, from kubernan (to steer or control). Cybernetics is the field of study that compares the control and communication systems of the body with mechanical or electronic systems of control and communication. It is about human control and control and communication systems and the electronic and mechanical systems designed to replace them. Therefore, cybersecurity is a shortened for of cybernetic security – the protection of electronic and mechanical systems of control and communication designed to replace human systems of communication and control from potential adverse event. The US CISA (2009) notes that "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information." Therefore, cybersecurity encompasses activities aimed at the protection of computer systems, devices from the theft and damage to hardware and software programs or electronic data, as well as the disruption or misdirection of services that they provide.

1.2 Research Problem

The agri-food sector has been involved in the adoption of information technology to manage production, processing, transportation, distribution and retailing of commodities and food products for decades. Agri-food supply chains are increasingly becoming interconnected as efficiency in communicating and controlling inventory at different stages in the supply chain enables effective achievement of customer satisfaction, enhance customer loyalty and improve profitability and competitiveness. The increasing networking of agri-food companies involves the sharing of massive amounts of data across computer networks. And this sharing creates the environment for cybersecurity risks and the necessity of pondering cybersecurity strategies.

It is important to observe that while the focus of cybersecurity has been on nefarious intents of criminals, some cybersecurity risks are accidents arising from carelessness on the part of individual employees across the spectrum of power in organizations. Whether they arise from nefarious intents or through negligence or carelessness of trusted employees, cybersecurity in the agri-food sector can disrupt organization's activities across their supply chains, put their reputation and goodwill at risk, and have direct significant impact on their financial health. It is for this reason that assessing the risks facing agri-food companies in the age of cybersecurity risks is appropriate and timely. Unfortunately, there is little to no work in this area in the literature. The imperativeness of bringing some focus to this problem is expected to help the agri-food sector develop a collective, systematic and strategic approach to the challenges (and opportunities) presented by cybersecurity.

1.3 Research Question

Given the foregoing problem, the question motivating this research is this: What is the various cybersecurity risk facing the US agri-food companies and how may they mitigate these risks? This question is driven by the need to classify the different cybersecurity risks to which the agri-food sector is exposed and developing a systematic approach to dealing with each of them. It is hoped that this research would raise awareness about the risks associated with cybersecurity in the agri-food sector and encourage those who have not yet taken steps to address these risks to begin taking it seriously.

The importance of acting on this challenge is that because of the increasing networking of organizations in the sector – from producers and their input suppliers to retailers and their customers – potential partner organizations are going to assess each other's security risks before engaging them in non-atomistic relationships. This implies that those without strong security systems in place will find themselves on the outside looking into structured supply chain relationships.

1.4 Research Objectives

From the foregoing research problem and research question, the overall objective of this research is to develop a comprehensive catalog of cybersecurity risks facing the agri-food sector with the view to developing pragmatic, effective and competitiveness-enhancing responses to them using existing and potential solutions. The specific objectives are as follows:

1. Explore the extent of cybersecurity risks in the US and extrapolate the cybersecurity risks facing the agri-food sector.

2. Classify the current and potential cybersecurity risks facing the agri-food sector and assess their potential implications on the US sector's competitiveness.
3. Develop a comprehensive strategy for enhancing the cybersecurity of the agri-food sector with the view of enhancing the competitiveness of US agri-food firms.

1.5 Overview of Methods

The research uses an extensive literature review to explore the extent of cybersecurity risks in the US. It uses a keywork and impact analysis to classify the identified risks into coherent groups. Using examples from other industries, it will assess the potential effect of these risks on the agri-food sector using simulations. Finally, it will draw on Kim and Mauborgne (2015) to explore strategic initiatives that may be employed by agri-food firms to not only manage their cybersecurity risks but thrive in an increasingly networked economy.

1.6 Outline of the Thesis

This chapter presented the background and justification for the research. The next chapter presents a review of the literature to address the first objective. It also presents the classification system and uses it to classify the identified cybersecurity risks facing agri-food firms. It provides an overview of the potential implications of these risks to the US agri-food sector's competitiveness. That chapter covers the second objective. The third chapter addresses the issue of dealing with cybersecurity, developing a typology of the areas that need to be covered. It focuses at its end on the steps that might be used to mitigate the identified risks cyber insecurity presents to the agri-food sector.

CHAPTER II: CYBERSECURITY LITERATURE – SELECTED OVERVIEW

In this chapter, an overview of the computer network usage and its attendant problems of cybersecurity are presented and discussed. The chapter also explores specifically the expansion adoption of internet technologies in the agri-food sector, exploring the transformational initiatives that internet of things (IOT) and other dimensions of the Fourth Industrial Revolution (4IR) are introducing to the sector and how the sector is positioning to succeed in this emerging environment.

The chapter is organized into four sections. The first presents an overview of cybersecurity risks in the US. The second addresses how these cybersecurity risks manifest in the agri-food sector. The third section traces the path that has led to this point and explore where the agri-food sector is going within the scheme of events happening in the general economy. The final section illustrates how the increasing connectivity across devices and organizations exacerbates the cybersecurity risks, arguing that disengagement is not an option if one seeks to secure and enhance competitiveness.

2.1 Cybersecurity Risks

There is no shortage of risks in the global environment these days, particularly in issues that concerns connectivity in the world order. With the tensions between the US and North Korea, China and Russia, the targets for cybersecurity risks may be divided into two broad groups: (1) Personal and commercial entities risks aimed at stealing information that may be deployed for the gain of those perpetrating the security breaches; and (2) Government entities for the sake of humiliating or controlling adversaries for political gain. In the second group is what has come to be recognized as cyber-terrorism. It is projected that

cybercrimes will cost more than $6 trillion by 2021, making it more profitable than all the global trade in illicit drugs combined. This estimate includes damage and destruction to data, lost productivity, theft of intellectual property, post attack disruption to the normal course of doing business, forensic investigation, reputational harm and restoration (Cybersecurity Ventures, 2019).

Cyberterrorism is a "premeditated, politically motivated attack against information and computer systems, computer programs and data that results in violence against non-combatant targets by sub-national groups or clandestine agents" (Tafoya 2011). The Center for Strategic and International Studies (CSIS) published a report on the subject of cyber-terror, which argued that it is "the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population" (Lewis 2002, 1). Lewis goes on to say this of cyber-terrorism: "the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information."

Social Engineering attacks: This is a skill set process that hackers use to psychologically manipulate businesses and people in general., in giving away sensitive information. A common form of this attack is phishing. It is a ticklish deceptive email that tricks the potential receiver in giving out sensitive and vital information.

Advanced persistent threat (APT): These are basically attack in which hackers or unauthorized users get into / infiltrate your network without your consent for a long period of time. The essence of this type of attack is to still company and individual data, here we

are talking about sensitive agricultural data, company trade secrets that competitors can use against you to have an edge over you. This type of attack is prevalent where there is high volume of information. It is in most cases to still data and not to harm the network.

Malware: This is a software that is designed to enable access into a network and cause damage without the knowledge of the authorized owner. There does exist various types of malware, Virus, keyloggers, worms, trojan horses, spyware, ransomware (Sykuta 2016). Some of these malwares do propagate themselves without user intervention. They start by taking advantage of any software vulnerability. Once a computer is infected, the malware begins to replicate itself throughout the network. It does come through network-based software, emails and websites. Some malwares pretend to be what they are not. There are situations where a software that is supposed to help speed up computer networks will disguise and then steal company trade secrets, delivering them to a remote intruder.

Viruses and worms can self-replicate and damage files and systems, while trojans and spyware are often used for surreptitious data collection. Ransomware waits for the opportunity to encrypt user's information (holding them hostage) and demanding ransom payment (hence the name). Release of the encryption code is only done upon receipt of payment, which is often demanded by done in cryptocurrency, such as bitcoin. Malwares are often distributed through legitimate looking emails or email attachments (Kaspersky, 2019).

Denial of Service (DOS): In this type of cyber-attack, the attacker's intension is to make the machine or network resource unavailable to intended users by indefinitely or temporarily disrupting services to a host connected to the internet. This is done by flooding

the targeted machine or resource with overwhelming request to overload system and deprive legitimate request from being fulfilled or accomplished. Distributed Denial of Service (DDOS) is even worse because it uses multiple systems to flood the bandwidth or resource of a targeted system, usually one or more web servers.

2.2 Possible Avenues for Cyber-Attacks and the Agri-Food Sector

Cyber-attacks may occur through various avenues in the agri-food sector. However, it is important to note that the agri-food sector is not unique in the way cyber-attacks are manifested. The four possible avenues through which cyber-attacks can occur are as follows: (1) Disruption of delivery; (2) The interception of confidential information; (3) Alteration of formulations; and (4) Tampering threats.

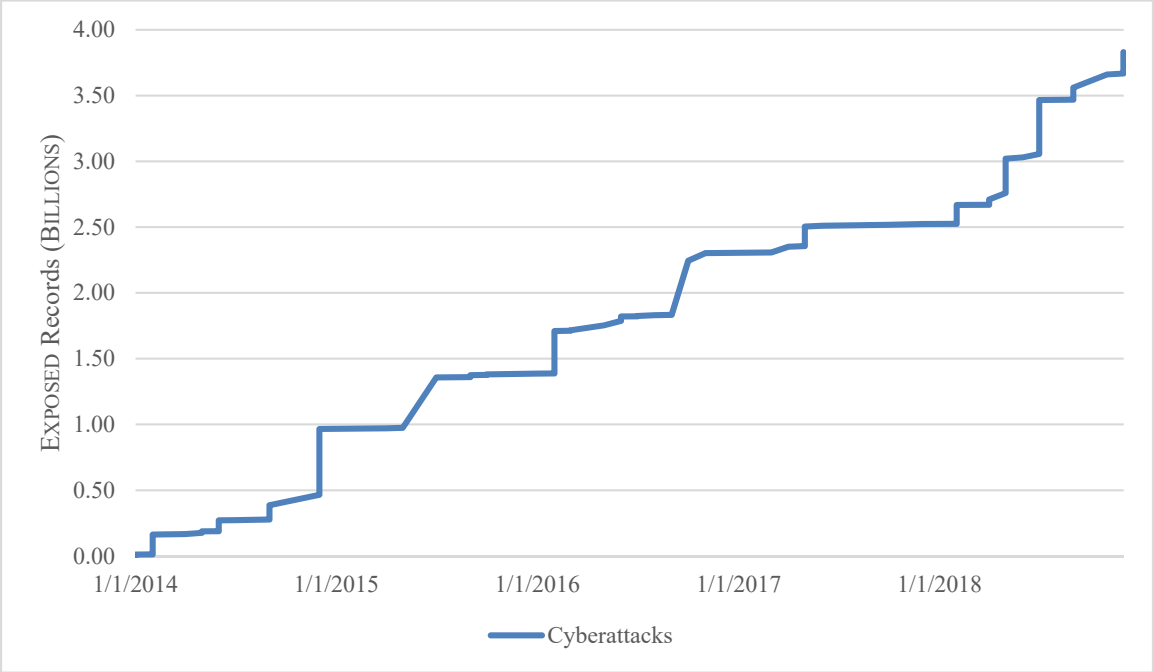
Disruption of delivery involves intentional actions taken to interfere with the physical or virtual delivery of products and/or services. In the cyber environment, this could occur by interfering maliciously with control systems and information systems to disrupt the delivery of products and services to clients or downstream partners of a supply chain. While physical threats to delivery of agri-food products through the supply chain have been minimal to absent to date, the risks in the cyber environment can be immense. By disrupting delivery through misdirection or misinformation, highly perishable agri-food products can be wasted, creating significant financial losses to companies on both sides of the delivery process. Likewise, such actions can engender mistrust in suppliers as credible and dependable, causing an erosion of confidence, which can carry significant reputational and business costs.

Disruption of delivery can also be used strategically in cyber warfare. For example, criminals or state agents working remotely to alter delivery location instructions can cause a lot of confusion in the supply chain. Imagine a small restaurant receiving on its dock a 56-foot trailer of milk that should have gone to a Club store in a location clear across the country, and that club store receiving a box of crackers that was meant for a consumer on the other side of the country. By aggressively undertaking these disruptions, the attacker creates confusion and panic even as it increases operating costs and reduces competitiveness across the sector. These issues are being contemplated by the Department of Energy and Department of Homeland Security as they pursue protection of the computer systems and networks upon which the delivery of electricity and other energy are delivered to distribution companies for onward distribution to consumers across the country.

Whenever a user is on a web page completing a form, there is a risk that someone interested in the information being provided might attempt to intercept its delivery to the intended recipient and capture it for their own use. Its value is often real because there is often ready market for such information, allowing the intercepting criminals to benefit almost instantaneously from their actions. Interception of confidential information also involves hacking into companies' computers to retrieve confidential information that are stored there. Information, such as credit card information, and client information such as social security numbers, have significant value to criminals who want to use them for incurring debt or procuring services in other people's names. These information theft activities form the foundation of identity theft, a crime that costs about $1,343 per victim and estimated to affect almost 20 million US residents in 2014 (Harrell 2017). Identity

theft was estimated in the Harrell paper to be increasing in all categories – credit cards, bank accounts, personal information, etc. Figure 2.1 is the cumulative trend of exposed records between 2014 and 2018. By the end of the data, nearly 4 billion records had been exposed in the US. These numbers do not include the US Government's exposure. Additionally, experts believe the numbers here presented are only a fraction of the true size and extent of the problem because many companies do not report their exposures.

Figure 2.1: Cumulative Number of Exposed Records in the US between 2014 and 2018 (Excluding Government)



Source: Bloomberg, 2019

Figure 2.1 includes confidential information harvested from the retail giant, Target, and the ag chemical giant, Monsanto. It includes Cambridge Analytica's harvest of more than 50 million user profiles from Facebook. Cambridge Analytica's approach was simple but

effective. They built a quiz app and used it to collect profile and other data from those completing the quiz as well their friends and their friends' friends who had nothing to do with the quiz. This illustrates how competitors may intercept information of commercial and competitive value and use them to their advantage in client acquisition and market share development (Norton, MacAfee). Examples of how this may be accomplished for commercial purposes were seen in the 2016 Presidential elections.

Alteration of formulation can present significant risks exceeding those presented by those already presented. Imagine a nefarious organization or individual altering the formulation for a pharmaceutical product in ways that cause harm to consumers using such products and hijacking the quality assurance process to mask the alterations. Depending on the objective of the individual criminal., the impact can be instant, rapid or very slow. The slower the impact, the longer it will take the authorities to discover the alteration in the product. Such a risk negates the warning the pharmaceutical companies put on their consumer-packaged goods – "discard if seal is broken". The risk occurs in the manufacturing process and through the quality assurance activities. The foregoing is feasible because of programmable logic controllers (PLC). These are industrial digital computers that have been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, robotic devices, or any activity that requires high reliability control and ease of programming and process fault diagnosis (Wikipedia).

This example of what can happen in the pharmaceutical industry can happen in food manufacturing industries as more of product formulations and production are automated through networked systems. Opportunities for cyberattacks, their nature and

extent, are driven by the objectives of the attacker. However, as suggested by Joshua Cooper Ramos in his book *Thinking the Unthinkable*, failing to explore the different combinations of the unthinkable puts the "good guys" in a reaction mode all the time, chasing the "bad guys." It is time for new and novel minds to explore radically dangerous scenarios as they build systems to protect the agri-food systems from the potential risks that cyber-attackers may use to unleash havoc on the food production, manufacturing and distribution system.

Data tampering is simply the changing (including insertions and deletions) of how a programming code is expected to behave. In lot of ways, it is biggest of all the cyber-attack threats. Tampering involves other activities, such as interceptions. The criminal intercepts an unprotected packet of instruction that is being transmitted over a network, and modifies its contents, or changes its destination address. The intruder can also introduce malicious instructions that can cause significant havoc for industries and governments. Since tampering begins with intrusion and then interception, it is important to think backwards and figure out how to prevent intrusions so that malicious tampering scan be prevented.

There is a subset of cyberattacks by cyber activist. These are the group that would disagree with a company's product or the method that a company uses to produce a product. Individuals or groups of this nature have the tendency to use hacking to attack and tannish a company's reputation, maliciously modify its automated processes, disrupt its operations and cause damage.

These attacks can be perpetrated from and in anywhere in the world. There is obviously no requirement for anyone involved in cyberattacks to even set foot in the facility that is being attacked. That makes it more frightening. Because of the foregoing, it will be proper to say that the agri-food industry has no choice but to guard against potential cyber-attacks. Unfortunately, it is not the case as would be expected, surprisingly. Several factors could be the reason why this is the situation as of now. They include a lack of awareness of the problem, incomplete and inadequate appreciation of the challenges, and connectivity loopholes, or inadequate security systems.

Let us begin with lack of awareness. Breaches in the food industries would not be noticeable initially, when compared to a machinery or equipment that is not functioning, or a flooring or roof in a factory that needs repairs. In most industries including the agri-food industry, protection of the computerized system resource wise is not in their priority list. They tend to pay more attention to budgets that pertains to productivity and improvement of food safety and quality before focusing on cybersecurity, particularly in companies that have never been attacked by hackers. This lack of focus towards cybersecurity can result to system vulnerability in the agri-food industry. Included in vulnerability of this nature is the operating systems that could be corrupted, insecure remote access portals, outdated firewalls and even employees that have little or no training whatsoever and not aware of the danger of potential risk as it relates to cyber-attacks.

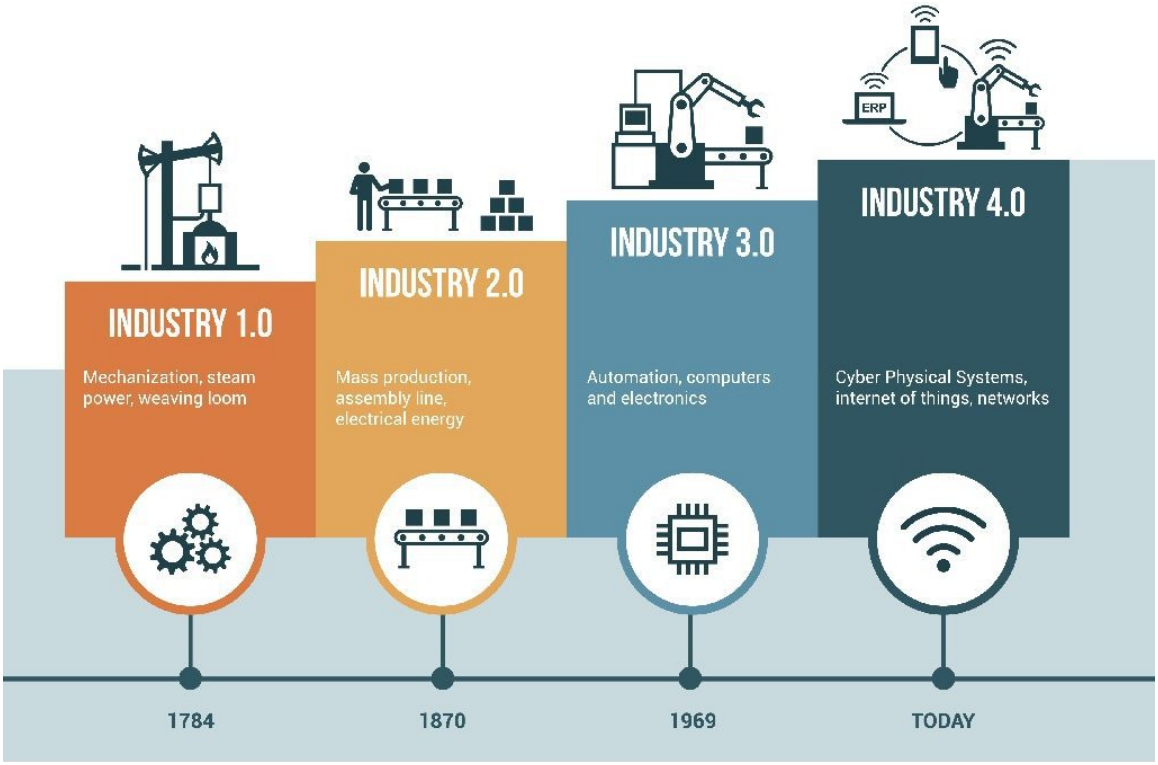
Another aspect of this lack of appreciation of the challenges is that firms that do have defense mechanisms in place against cyber-attacks, tend to often pay more attention to their database systems, and overlook the possibility of professional hackers utilizing

innovative methods and indirect access methods, through third party to bypass the gates (entry point) to gain access to company secret data that could be damaging to an agri-food firm being attacked. These are systems the concerned firm had assumed to be secure.

Risk exposure to cyber-attacks also emanate from the assumption that processes of protecting and recovering networks, devises and programs from any form of cyber-attacks are intact. Cyber-attacks are dangerous to organizations, their consumers, and employees. These attacks are designed to access and destroy sensitive data or extort money (Norton). They can damage business practices and their reputations.

The connectivity in the agri-food sector includes control over the means of information, transportation of physical goods and services as well as intangibles, such as computer codes for equipment and facilities. This have become increasingly ubiquitous as organizations operate in the Fourth Industrial Revolution O Industry 4.0 (Figure 2.2). In this industrial era, which is reputed to have started around the turn of the current century, organizations are operating on cyber physical systems. It involves connected systems that utilize big data and augmented analytical processes to achieve business objectives.

Figure 2.2: Progression of the Industrial Revolutions and their Main Characteristics



It uses augmented reality and cloud computing to provide insights into customer decisions and preferences, helping organizations improve customer satisfaction. The adoption and use of smart sensors, location detection technologies, mobile devices and multilevel customer interactions and profiling to improve supply chain effectiveness and value creation is the expected outcomes. It involves the digitization of products such that manufacturing can be done on demand and customized using such technologies as 3D printing. Transparency in business models and improved interactions with customers and suppliers are at the core of the business models under 4IR. And it is also in this enhanced connectivity and transparent interactions that organizations become vulnerable to cyber-attacks and cybersecurity risks.

The critical cybersecurity risks facing the agri-food sector are recognized by those charged with overseeing the country's systems and cybersecurity. For example, the Department of Homeland Security has labeled the agri-food sector among the 16 national critical infrastructures. Thus, just as technological advances have enhanced productivity, and provided the agri-food sector with new opportunities, it is here argued that increased connectivity and the characteristics of the 4IR present heretofore unimagined risks to the sector. For example, computer usage at the primary production level has increased significantly over the past decade, with most farm information providers delivering via smart phones and other connected devices. That is how the connectivity exposes the industry to these risks. However, most of these risks are known and have been researched in other industries. The challenge is taking the results of those research products and adapting them to fit the unique characteristics of the agri-food sector.

2.3 Cybersecurity in the Agri-Food Sector

The pace at which technology is evolving is unbelievably fast and amazing, the agri-food industry is constantly faced with adoption choices. It is vital to examine the technologies that are been used and how they are been implemented in various industries, particularly the agri-food industry. As these technologies continue to proliferate, the agri-food industry and the billions of people it serves globally are increasingly at risk from cyber-attack threats. (Molly et al., 2019).

It is a known fact that agri-food industries are becoming dependent on information networks. These are the same networks that have been recognized to be responsible for the new risk in nearly all facet of modern life, resulting from cyber vulnerabilities that may potentially have global scale impacts in different dimensions. For example, John Deere

combines are now connected to the networks, allowing operators to remotely check engine conditions and operational productivity (Schemper 2014).

It is also important to be aware of one of the reasons behind this competition for technological competition in agri-food sector, it is because of the economic backdrop, farmers are now been pressured to pursue higher per-acre productivity and a lower operating cost to stay in business (USDA/ERS, 2017). Because of the pursuit in achieving these goals and the challenging market situation with the environmental factors, this has resulted to increase in the demand for highly connected smart devices in the agri-food industry. This is applicable to its supply chain, distribution systems, smart production and smart market systems, thus opening and increasing channels for cyber-attacks.

These technologies we now call "precision agriculture" is where smart devices integrate with smart markets, enabling timely allocation and more precise farm resources in times of growing, harvest and transportation of agricultural products off the farm. Precision agriculture has been confirmed to raise production efficiency. (FAO,2017). By its improved and efficient use of inputs (water, crop nutrients, seeds, pesticide, herbicides, fertilizer and others), production efficiency is raised, thus increasing production per acre. (Clearly, 2017). This is obviously a game changer in the agri-food industry. With all that been said, it is important to realize that any smart technology, no matter how good it is, if not properly secured, also inclusive is smart markets, if not monitored severely may result to disaster. That is to say that hackers will take advantage of the lapses and cause havoc to food distribution by manipulating the system. Just to mention a few that could be manipulated, robotic milkers, autonomous, agricultural planters, harvesters, cultivators, the

application of herbicide, pesticides, fertilizer, driver less tractors and trucks for delivery that are in the making etc.

All these technologies are geared towards enabling farmers to be more focused on managing and planning their activities, from planting, cultivating, and harvesting to transportation, delivery, payment and processing of their product. (Brown, 2018).

U.S agri-food is routinely studied and adopted around the globe. This makes the translation and application of data-driven technologies for autonomous systems, precision agriculture, data recording, yield large data sets of economic and bio-based information for agri-food industry. (Sykuta, 2016). Because of the high throughput processing nature, data management and integration and other management of computer-based management of these data, there have been advances in decision processes, increase in efficiencies, and increase in output within the agri-food industry. Notably, information of this nature is susceptible to theft, ownership policy challenges and cyber-attacks, because users are not aware to the potential vulnerability or lack of training in respect to effective security and protection strategies. (Sykuta, 2016; Bogosian et al., 2018). There is the possibility that unprotected and even weakly protected systems in the agri-food industries will obviously be susceptible to intrusions and unwanted attacks through surveillance and tendency for potential malicious cyber- attacks. These cyber threats could include unwanted access to analytical technologies, vital data, access to systems, and the improper use of stolen information to cause harm in areas of research, production, processing , advanced breeding, high performance livestock, high yielding and specialty agricultural crops , bio technology

advancement and even big data analyses etc.(National Academics For Sciences, Engineering and Medicine, 2014).

It is good to realize that the agri-food industry also applies to military food production, involving manufactured packaged meals for soldiers which has the tendency for sabotage. (Colbert et al., 2018). Attackers don't have to know the in depth of the food manufacturing process, all they need to know is the technical methods needed in exploiting the machinery or the process that is in place, such as the ability to lower the temperatures on meat cookers before packaging remotely (Colbert et al., 2015).

There has been a paradigm shift since the incorporation of cyber-based technologies and data-based solutions in farm production, food processing, transport goods, supplier industries, marketing sales, communication with consumers. (Boghossian et al., 2018). Also to be aware of, is the use of cloud based storage of large data sets, the use of open sourced or internet and cloud based software and cooperate based management of proprietary software, these have each increased the chances of unauthorized access to vital data in the agri-food industry. The use of research laboratories, biological and genetically analyzed technologies are very widespread for the evaluation of food quality, animal and plant health inclusive, which are enhancing the rate of new products. (United States Department of Agriculture National Institute for Food and Agriculture, 2016; Wintle et al., 2017). All these can create cyber-attack threats which can in turn harm public trust in the industry. When the above is the case according to strategist, they may cause more harm than the actual threat itself. (Wintle et al., 2017).

The FBI (2017) has warned against the increase threat of cyber-attacks in the agricultural industry towards the following:

> *The targeting by cyber criminals towards seeking to steal farm level data in bulk. Also targeted by these cyber thieves is the aggregated and analyzed data to exploit U.S agricultural resources and its market trends.*

Also included in the report is the targeting of farm level equipment that collects data about soil content and past crop yields, including planting recommendations. Additionally, the report identifies hacking of public worldwide climate and crop data that is used to design visualization tools for farmers. Also, in their agenda is the susceptibility to ransomware and data destruction. Finally, drone manufacturers that are focused on offering low pricing structures for farmers by using systems that are interoperable with networked devices with poor cyber security protections.

As the agri-food industry increase its reliability on digitized data and the increase in the sophistication of hackers and cyber threat mode of operation increasing, most major agri-food industry and farm equipment providers are investing in stronger cyber security. Monsanto is amongst companies in this sector working to improve its cyber defenses after it had acquired farm analytics, the climate corporation had a cyber-attack in 2014. (Homeland Security Newswire, 2014). It was also reported that the agri-food sector will be facing increased cyber-attack threats, because of the growing adoption services and that they are collecting and analyzing data from farms, inclusive is soil content and the crop yields and other planting recommendations. (Wall Street Journal., 2015).

The US Council of Economic Advisers (2018) did report that the agricultural sector had 11 cyber-attacks incidences in 2016. Many security experts believe that the integration of the IoT (Internet of things) with combination of blockchain technology, which can create a verified, distributed ledger will be capable of improving security, which will enable proper and more reliable tracking in relation to the smart devices/systems. (Petracec, Nelson, 2018). This makes it more difficult for hackers to break in. This is possible because the possibility of a single point failure is eliminated because of the cryptographic encryption technology distributed across many verifying nodes that is entailed in the storing of the shared data in the blockchain (Banafa Ahmed, 2016)

CHAPTER III: DEALING WITH CYBER SECURITY THREATS

This chapter presents some strategic approaches that may be used to address the challenges associated with cybersecurity presented in the preceding chapters of this thesis. The chapter is organized into four sections. The first and the second sections look at dealing with the threat to confidentiality and to integrity. The third section looks at addressing the threat to availability. The final section explores the broader challenges of mitigating cybersecurity threats, serving as a summary of the discussion presented in the chapter.

3.1 Threat to Confidentiality

Data privacy is very important in precision agriculture implementation and agri-food industry in general. It is vital for farmers to be protective of their information, such as land prices, yield data, herd and crop health. Any form of tampering or loss and even misuse of these data can have a catastrophic effect to the emotional and financial impacts on farmers. There is also the potential for reputational negative effect against equipment and software manufacturers. Other threats in this category include the following.

3.1.1 Unfairly unauthorized use to confidential data

Confidential information/data could be used negatively against farmers on the commodity market, which would have a damaging effect. There has been evidence of data sales on the black web market online. There also exist sales to hedge funds and commodity brokers in the past.

3.1.2 Publishing confidential information that could be damaging from suppliers

The possibility and potential by a supplier to publish information such as market data and confidential pricing of famers could be disastrous to any business and agri-food industry. This can lead to loss of trust and exodus of customers, resulting in drop of profit margin. An example of this type of attack is the incidence with Sony pictures in 2014.

3.1.3 The intentional data theft and/ unintentional data leakage

Occurrences of this nature has been on the increase in the industry particularly in relation to mobile apps, that are designed to support farmers. Most of these apps were built by university extension programs who do outsource their programming, also startups that may not be patching for updates. User agreements, privacy controls, third party applications, systems update, and others are not properly done. Some of these apps are designed intentionally to still vital data. This is a threat not to be taken likely.

3.2 Integrity

The agri-food industry regarding precision agriculture has moved tremendously into smart farming. Massive sensors are been built both in crop and livestock sectors respectively. Of vital importance, is the collection of data, and its exploitation is considered a valuable tool in assisting real time farming and livestock decisions. Because of the quick pace precision agriculture has adopted robotics, machine learning, edge computing, equipment automation, there has been a sharp increase to threats of data integrity like has never been seen in the agri-food industry. This is to be taken seriously.

3.2.1 Rogue data introduction into network

Smart sensor implementation is deepest in crops like vegetables, fruits and nuts. These sensors are connected through blue tooth, WI-FI networks, cellular and they mostly

rely on edge computing in making decision at the source. Rogue data introduction could result in faulty sensors, which could bring about under or over watering of crops, in the process, destroying the crops. The same also applies to livestock herds been managed in farm buildings. In this scenario faulty sensors could disrupt HVAC systems, that could result to adverse health conditions that could result to death of the animals.

3.2.2 Falsification of data to disrupt both crop and livestock

An unapproved genetic modification can cause massive economic disruption, real impact on food security, complex foreign trade issues. It does take quite some time and huge resources to confirm and control disease outbreak in livestock. It is done through field and laboratory work. A malicious hacker can manipulate critical data that can wipe out a whole herd through disease outbreak. Same scenario applies to crop as well through improper mixing of GMO products into the supply chain, which can result to crop diseases and destruction.

3.3 Availability

Threat to availability is simply put the disruption of agricultural food, production and supply. Threat to equipment availability can result from cyber related issues and natural disasters. Crop and livestock operations are reliant on this equipment. Any threat to equipment availability can be catastrophic.

3.3.1 Timing of Equipment Availability

It is to be noted that for every crop there is a window of time to plant and to harvest which implies also that all machinery for these operations must be in working conditions. Unavailability of machinery for the appropriate timing because of malicious hackers could be disastrous and detrimental. Equipment's that are vulnerable to cyber-attacks can be

easily manipulated in their thousands at the same time, or even inappropriate patches can lock up machines that are supposed to be operational., resulting in downtimes.

3.3.2 The Disruption to navigational., positioning and time systems

The United states protected spectrum close to the global positioning system (GPS) is getting overcrowded and it is been released for 5G broadband signals, with the tendency for signal disruption. Farmers do face signal loss because of the overcrowding. This is not good for precision agriculture.

3.3.3 Disruption to communication networks

The agri-food industry is built on distributed sensory networks that are involved in data transfers of high volumes. Famers do rely on Bluetooth, Wi-Fi networks and cellular and USB drives to manually transfer data. It is to be noted that rural communications networks are major week points for precision agriculture and thus poor connectivity results.

3.3.4 Foreign Supply Chain

It is important to know that foreign manufactured equipment could be remotely disabled in large numbers through backdoor access from firmware, through malicious code that is sent to the equipment during planting or harvest seasons to cause damage.

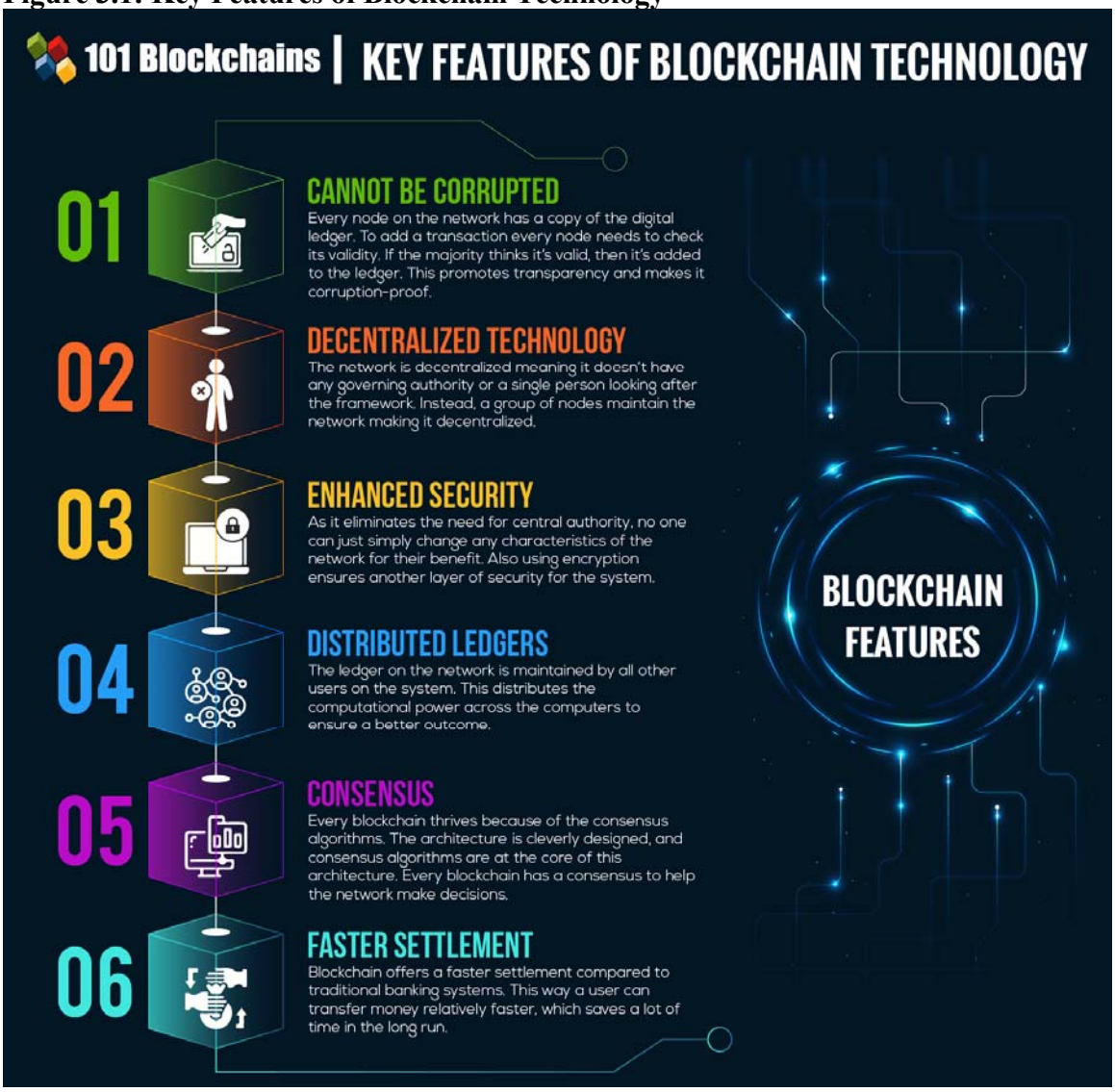
3.4 Mitigating Cybersecurity Threats

Thus far, the generic approaches to addressing cybersecurity threats have been presented and discussed. In the remaining sections of this chapter, the specific technologies and innovative solutions to dealing with these threats in the agri-food sector are presented. It also explores the opportunities that may be seized because these threats exist in the sector.

3.4.1 Block Chain

Blockchain is defined as a data structure making it possible for participants in the chain to create immutable ledgers to record their transactions and track their assets across the network (Laurence 2019). The network assets may be tangible or intangible. Tangible assets are physical goods, such as grain, livestock, trucks, etc. and intangible assets include branding materials, cash, intellectual property, social network, etc.). Blockchains allow its partners to record and track anything of value to them in a way that cannot be altered once it has been recorded, and in a way that is transparent to all partners. These are digital information that are stored in public database. They are growing list of records called blocks that are basically linked to Cryptography. Each block contains a cryptographic hash of previous block, a time stamp transaction data. The critical features of blockchain technology is summarized in Figure 3.1.

Figure 3.1: Key Features of Blockchain Technology



Source: 101blockchains.com

Blockchains provide solutions for product wastage, Food fraud, supply chain visibility and management. It obviously does help in planning and executing of harvesting and storage efficiently and delivers entirely new use cases. It is essential that blockchains be in place for several reasons. Block chains enable traceability in supply chains, producing real time logistics data accurate, with speed and security. An implemented blockchain will

go a long way in addressing the challenges presented above – food water, unknown origins, food fraud, lack of traceability, inefficient payment, lapses in policy (e.g., subsidy management. It allows for the development of the confidence in the knowledge that every asset in the supply chain, because it is linked to the IoT, can be tracked and assigned unique identification, recorded in the system in a way that is immutable, hack-proof and easy to read in a distributed ledger format.

These blockchain ledgers can record and update the status of crops from planting and harvest to storage and delivery. They can record and update the status of livestock from insemination, pregnancy conditions, delivery and delivery situations, to feeding and delivery for processing. That the information is tacked and recorded in an immutable system allows it to have the integrity regulators need to access regulatory compliance.
It is also good to know that blockchains are based on shared ledgers or DLT (Distributed Ledger Technology). DLT is one big ledger in the cloud, putting it simply. The ledger contains records, transaction details, and information called blocks. These blocks, as they are called, are immutable and tamper proof. The data in these blocks are hard to alter or hack. Anyone can but put anything of value on the blockchains because they are incorruptible trust. That is why it is possible for farmers, consumers and retailers to register and share tangible information with maximum safety, transparency and speed. The data that is inputted is visible to all the elements in the blockchain. There is the option to either approve or reject the information entered. Once data entered is validated, it gets recorded into blocks, which are then organized in blocks chronologically and cannot be altered by anyone. This enables

farmers to get instant data about the seed quality or feed availability, get situation information on market conditions and payment completion (Zebi,2018).

3.4.2 Back up Files

Ensure files are backed up regularly to prevent disaster in case of a cyber-attack. This is also a measure taken in case there is a successful attack that requires the cleaning of your whole devices to enable reload information from the storage back up. It is important to always update devices. These routine updates contain patches that will fix security short falls.

3.4.3 Do not open unknown emails

Do not open email attachments from sources that are unknown. This also applies to links from emails that come from unfamiliar sources. A very easy way of attack is pretentious emails, disguised to be coming from someone you know. It is important not to provide vital information to sites you do not trust. Ensure to check URL if it has the secure lock emblem that identifies a secure site. Make sure it has “https:// address, don’t enter sensitive information in a URL that only has http://. Without the (s) at the end is not safe.

3.4.4 Run up to date antivirus software

Ensure to install reputable antivirus software application. It does guard against known attacks that are malicious. It will help to remove, detect and quarantine various types of malware. It is good to note that it does not function properly on zero-day exploits (exploits with no solution in place to resolve issue) and polymorphic viruses (uses a polymorphic engine to mutate while keeping the original algorithm intact. The code does change itself each time it runs, but the code function does not change.

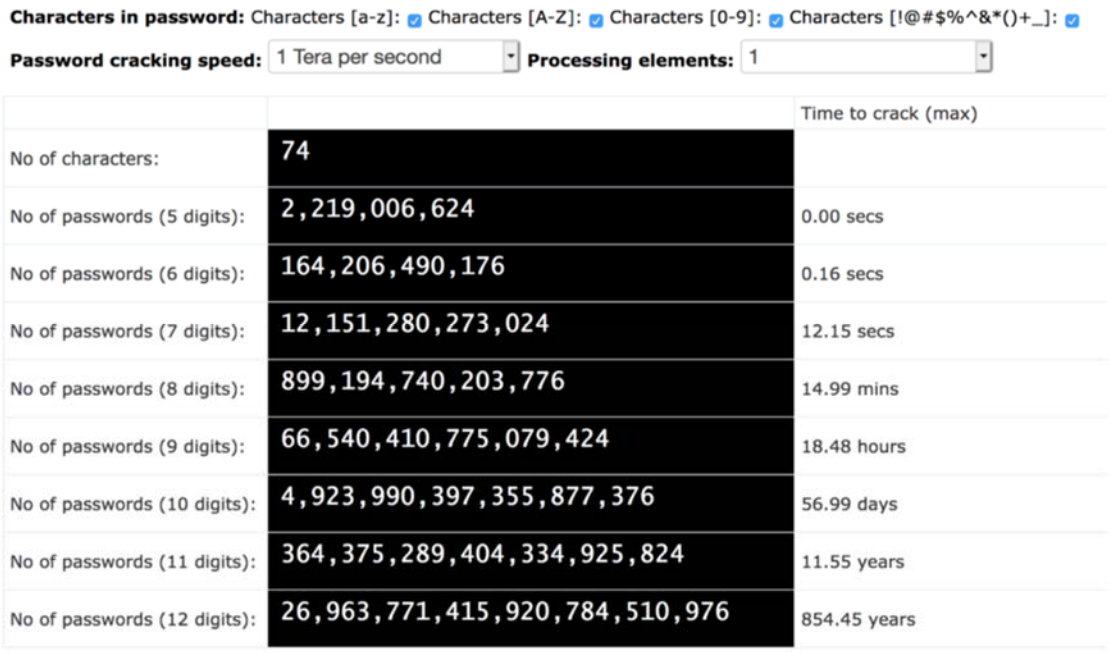
3.4.5 Password management

Make sure to change default name and password that are offered when operating in a network environment. Malicious hackers already know these default and password names. They can therefore work to access them quickly. Ensure to change them as soon as possible to uniquely strong password.

Using a strong password makes it difficult for attackers to guess or decrypt the password. Attackers may attempt to get passwords through phishing attacks and keylogging, surfing and mass data breaches. Keylogging is a software that tracks the keystrokes on a keyboard as they are entered in a covert manner. When installed on your system, keylogger captures passwords as they are being entered. SentinelOne notes that data breach approach to password access plain password dumps are loved by cybercriminals. The strength of passwords is controlled by two requirements: difficulty to crack or decrypt; and easy to remember.

Strong passwords are those that are difficult to crack and easy to remember by the owner. The observation is that the shorter the password, the easier it is for criminals to crack it. The figure below shows the time it takes to crack passwords given their lengths. It is estimated that passwords of less than 10 characters are easy to crack. For example, a six-character password drawn from a 74-characterset, which covers numbers, special characters, lower and upper cases, is crackable in less than one-twentieth of a second. However, a 12-digit password will take more than 854 years to crack. Hackers use computers that can run automated scripts in their search for passwords. But the more difficult it is, the most ardent criminal recognizes the benefit-cost of undertaking these ventures.

Figure 3.2: Cracking Time by length of Password



Characters in password: Characters [a-z]: Characters [A-Z]: Characters [0-9]: Characters [!@#$%^&*()+_]:

Password cracking speed: 1 Tera per second **Processing elements:** 1

		Time to crack (max)
No of characters:	74	
No of passwords (5 digits):	2,219,006,624	0.00 secs
No of passwords (6 digits):	164,206,490,176	0.16 secs
No of passwords (7 digits):	12,151,280,273,024	12.15 secs
No of passwords (8 digits):	899,194,740,203,776	14.99 mins
No of passwords (9 digits):	66,540,410,775,079,424	18.48 hours
No of passwords (10 digits):	4,923,990,397,355,877,376	56.99 days
No of passwords (11 digits):	364,375,289,404,334,925,824	11.55 years
No of passwords (12 digits):	26,963,771,415,920,784,510,976	854.45 years

Source: Sentinelone.com

To defeat cybercriminals, then, passwords must have maximum entropy, and unique to each transaction site. Using passwords that are easy to remember but difficult to crack is a good rule to follow. Difficult to crack passwords have, as noted above, 12 or more digits and include random combinations of letters (both upper and lower cases), numbers and special letters. SentinelOne suggests that passphrases are a lot easier to remember and are more difficult to crack if they are structured properly. Consider the example they give: NotInA(1)Month=[31-Days]Of*Sundays*. This 35-character passphrase and is a lot easier to remember than this 12-character string, l7aHPQ9-*=[9)(, which contains the same special characters. The passphrase is daunting for hackers and yet easy to remember. Finally, turning on two factor authentication (2FA) or similar authenticator protocols can improve security even when passwords are inadvertently

cracked. These 2FA protocols are methods that confirm identities using a combination of two different factors, such as something they know, something they have, or something they are. The commonly used is a password plus a code that the site administrator sends to the user via text message on their phones.

3.4.6 Install firewall and closed unused ports

Firewalls help keep out some malicious traffic before they get to computer systems. They also restrict outbound unnecessary communications. Implementing multi-factor authentication, such the 2FA protocol, can make it difficult for penetration to occur through firewalls. It is important to remember that attackers are very good at exploiting weak authentication. Monitor incoming and outgoing data: use intrusion detection and preventions system to monitor incoming and outgoing traffic. This will detect unusual traffic and block unknown suspicious IP addresses.

At the software level, ports identify specific processes and provides access to specific network services. The most common port protocols are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). Port numbers are associated with IP addresses of hosts and the protocol type. Open ports, therefore, allow communications with the network to occur. When ports are not in use, it is good security practice to close them. Unused ports that remain unclosed may also not be properly monitored.

3.4.7 Employee training and education

There should be continuous training of employees to inform and remind them of current social engineering tactics and threats. Use of VPN (Virtual private network) for remote login capability. Incorporate cyber security into agri-food safety and defense culture.

3.4.8 BYOD

Bring your own device (BYOD) is a common practice where participants in meetings or working at a site or engaged in similar other activities are encouraged to bring their own devices, which they then connect to the network via Wi-Fi or similar connections. Devices often store network information, often for the simple reason of reducing time and increasing convenience. However, if those devices are compromised, those stored data may still be available, allowing the thieves to gain access to the network. These devices could be mobile phones, personal computers and tablets or storage devices such flash or USB drives.

For employees, allowing them to work on their own private devices could position them to have company information and data stored on those devices. Should there be a fall out between them and the company, they could use the network access codes on those devices to penetrate the system and cause havoc. They can copy company information, take photos of documents and share them or sell them to competitors, or even use them to black mail the company. The 2013 case of Bradley Manning, the US military private who was convicted for providing vast amounts of military and diplomatic files to WikiLeaks, is a case in point. In his case, he felt his employer, the US Government, was not being transparent to the American people, and took it upon himself to leak what he considered embarrassing information to the public. See the report of the case by the New York Times' Charlie Savage, titled "Soldier Admits Providing Files to WikiLeaks" on February 2013 at https://www.nytimes.com/2013/03/01/us/bradley-manning-admits-giving-trove-of-military-data-to-wikileaks.html.

3.5 Conclusion

The agri-food sector is core in the American economy. While the sector faces numerous threats, such as production and market risks, its increasing participation in computer mediated information networks introduces it to newer forms of risks. While these risks are not new, they are to the agri-food sector, especially its upstream components of commodity production. For example, precision agriculture and other technologies, which involve collecting massive amounts of data from farmers and storing them in the cloud, present novel challenges about ownership, security, protection and access. Protecting the stakeholders of the agri-food sector from the threat of cyber-attacks is critical in ensuring the continuity of the agri-food industry. Furthermore, as stipulated in the recommendations above, the need for continuous education and the training of staffs cannot be over emphasized enough. Network device upgrades and updates are essential for the safety of the networks.

Because of the vulnerability of the agri-food industry to cyber-attacks, it is recommended that firms have in house trained cybersecurity professionals scouting their systems for weakness and maintaining their security software. There should also be both intrusion detection and prevention systems in place to constantly monitor network traffic for unusual traffic. It is also good to know that any agri-food company that has improved cybersecurity measures in place, with the new technologies will have better stand against competitors. This will allow it to create more value for its customers and others in the supply chain, enabling it to enhance its competitiveness.

REFERENCES

Adviser, The Council of Economics. 2018. “The Cost of Malicious Cyber Activity. “White House. February. Accessed November 3, 2019. Whitehouse.gov.

Agricultural Giants Boost Cybersecurity to Shield Farm Data, 2014. Interviews with Agricultural Industry Experts. Online: Wall Street Journal.

Agriculture, USDA National Institute for Food Agriculture. 2016. “Results of idea Engine Stakeholders Input.” NIFA Assessed January 7, 2020. www.nifa.usda.gov.

Banafa, Ahmed. 2016. “BBVA” BBVAopenMind. December 21. Accessed March 13, 2020 bbvaopenmind.com.

Boghossian, A, S. Linsky, A Brown, P Mutshler, B. Ulicny, and L Barrett. 2018. *Threats to Precision Agriculture, Dept of Homelland Security.* Accessed January 7, 2020. www.dhs.gov.

Brown, M. 2018. "Smart Farming-Automated and Connected Agriculture." *engineering.com.* May 15. Accessed January 24, 2020. www.engineering .com.

Bunge, J. *Agricultural Giants Boost Cybersecurity to Shield Farm Data".* Interviews with agricultural industry experts, Wall Street Journal February 19, 2015. Available at https://www.wsj.com/articles/agriculture-giants-boost-cybersecurity-to-shield-farm-data-1424380098.

Clearly, David. 2017. The Nature Conservancy. March 29. Accessed December 17, 2019. www. Nature.org.

Colber, E, D. Sullivan, K. Wong, and S. Smith. 2015. "Red and Blue Teaming of a US Army SCADA." *U.S Army research lab thechnical report* AL-TR 7497.

Colbert , E, D. Sullivan, K. Wong, and S. Smith. 2015. "Intrusion Detection Capabilities for US Army SCADA Systems." *Information Packet. US Army Research Lab technical report.* ARL-TR 7498.

Food and Agricultural Organization (FAO), 2017 “The Future of Food and Agricultural : Trends and Challenges”. www.fao.org.

Harrell, E. 2017. Victims of identity Theft, 2014. Washington, DC: US Department of Justice, Bureau of Justice Statistics.

Homeland Security Newswire. 2015. "Agro Cyber Vulnerability : U.S Farming Sector Increasing Vulnerable To Cyberattacks." *Homeland Security.* February 20. Accessed February 19, 2020. homelandsecuritynewswire.com.

Jahn, Molly M. 2019. Cyber Risk and Security Implications in Smart Agriculture and Food System. White, Wisconsin: Jahn Research Group.

Kaspersky, 2019. Kaspersky.com. Assesed February 10, 2020.

Kim, C., and R. Mauborgen. 2015. *Blue Ocean Strategy: How to Create Uncontested Markets and Make the Competition Irrelevant*. Cambridge, MA: Havard Business Review Press.

Laurence, T. 2019. *Blockchain for Dummies, 2nd Ed*. Holboken, NJ: John Wiley & Sons, Inc.

Lewis, J. 2002. Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats. Washington, DC: Center for Strategic and international Studies.

Mata. F.J., W.L Furest, and J.B Barney. 1995. "Information Technology and Sustained Competitive Advantage: A Resource-Based Analysis." MIS Quarterly 487-505

Medicine, The National Academies of Sciences Engineering and. 2014. *Safe Guarding Technology in the Bioeconomy.* Workshop, Washington DC: Board on chemical Sciences and Technology and the Board on life Sciences.

Morgan, S.. 2019. "Global Cybersecurity Spending Predicted to Exceed $1 Trillion from 2017 to 2021." *Cybersecurity Ventures.* June 10. Accessed February 2, 2020. cybersecurityventures.com.

National Institute for Food and Agriculture, USDA. 2016. "Results of "Idea Engine" Stakeholder input." *NIFA.* Accessed January 7, 2020. www.nifa.usda.gov.

Nelson, Patracek. 2018. "Forbes." Forbes website. July 18. Accessed March 13, 2020. www.forbes.com

Nicole C.K. James. 2018. "Cyberterrorism: How Food Companies Are Planning For Threat Of Cyber Cyber Security Risk." *Food Quality And Safety.* May 18. Accessed November 25, 2019. http://www.foodqualityandsafety.com.

Schemper, J.K 2014. Efficiency of combine usage: a study of combine data comparing operators and combines to maximize efficiency. Manhattan, KS: Kansas State University MAB.

SentinelOne. 2019. SentinelOne Blog. February 10. Accessed March 2020. https. //www.sentinelone.com/blog/history-of-cyber-security/.

Sykuta, M.E. 2016. "Big Data In Agriculture, Property Rights, Privacy And Competition In Ag. Data Services." *International Food and Agribusiness Management Review. Vol 19* 57-74.

Tofoya, W. 2011 “Cyber Terror. “Law Enforcement Bulletin.

Verizon. 2013. Data breach investigation report. Accessed February 12 2020. http://tinyurl.com.

Wintle, B.C, C R Boehm, J C Molloy, P. Millet, and L Adam. 2017. *A Transatlantic Perspective On 20 Emerging Issues In Biological Engineering.* doi, elife.

Zebi, (2018) “ Medium.” Medium.com. June. Accessed March 13, 2020. www. Medium.com.